Northwestern Journal of Technology and Intellectual Property

Volume 18 | Issue 3 Article 2

Spring 5-30-2021

THE GENETIC PANOPTICON: GENETIC GENEALOGY SEARCHES AND THE FOURTH AMENDMENT

Genevieve Carter

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

THE GENETIC PANOPTICON: GENETIC GENEALOGY SEARCHES AND THE FOURTH AMENDMENT

Genevieve Carter

May 2021 VOL. 18, NO. 3

Volume 18, Number 3 (May 2021)
Northwestern Journal of Technology and Intellectual Property

THE GENETIC PANOPTICON: GENETIC GENEALOGY SEARCHES AND THE FOURTH AMENDMENT

Genevieve Carter

ABSTRACT—

I. INTRODUCTION

On July 7, 2010, Los Angeles law enforcement arrested Lonnie Franklin, known colloquially as the Grim Sleeper, for the deaths of ten women in the Los Angeles area dating back to the mid-1980s.[1] In the Grim Sleeper case, law enforcement widened the parameters within the FBI's

[1] Greg Miller, *Scientists Explain How Familial DNA Testing Nabbed Alleged Serial Killer*, SCI. (Jul. 12, 2010, 1:18 PM), https://www.sciencemag.org/news/2010/07/scientists-explain-how-familial-dna-testing-nabbed-alleged-serial-killer# [https://perma.cc/577A-JZ2U].

Combined DNA Index System (CODIS) to find a familial match with Franklin's son who had been arrested years prior on unrelated charges.[2] The practice of widening the parameters of CODIS to find partial and familial matches to cold cases and other investigations was approved by the FBI in 2008, and has since been explicitly adopted by twelve states.[3]

Familial DNA searching within CODIS is not new, but consumer DNA testing products like 23andMe[4] are poised to offer a powerful new tool in crime fighting.[5] Today, consumer DNA databases are on track to host 100 million samples in the next two years.[6] AncestryDNA sold over $1.5 million worth of test kits in 2017 on Black Friday alone.[7] Unlike CODIS, the companies' individual privacy policies regulate access to these databases. Without any government oversight, the rise of private consumer genealogy databases in recent years has provided law enforcement with the ability to search these databases for matches to cold case DNA that has been sitting in evidence rooms for decades. While law enforcement is rarely granted access to search privately owned consumer DNA databases, consumers retain the right to download their DNA profiles from these private databases and upload them into public databases in search of family relations. These databases are free to use and allow individuals to volunteer their genetic information to find familial connections. They also allow individuals to affirmatively opt-in to use their DNA samples in fighting crime.[8] Since 2018, these consumer databases have led to the arrests of nearly three dozen people for violent crimes and cold cases.[9] In every case, those charged with a crime never actually uploaded their own genetic

---

[2] *See id.*

[3] *Id.*

[4] 23AndMe is a personal genomics and biotechnology company best known for providing direct-to-consumer genetic testing in which consumers provide a saliva sample that is analyzed in a lab. Other popular databases include Ancestry.com and FamilyTreeDNA.com. *See generally* ANCESTRY, https://www.ancestry.com/ [https://perma.cc/7XLP-2DYK] (Ancestry.com is a DNA test service provider); FAMILYTREEDNA, https://www.familytreedna.com/ [https://perma.cc/7XLP-2DYK] (FamilyTreeDNA is a DNA test service provider).

[5] *See* Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV.: BIOTECH. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/NX3Y-N7JM].

[6] *Id.*

[7] Megan Molteni, *Ancestry's Genetic Testing Kits Are Heading for Your Stocking This Year*, WIRED: SCI. (Dec. 01, 2017, 07:00 AM), https://www.wired.com/story/ancestrys-genetic-testing-kits-are-heading-for-your-stocking-this-year/ [https://perma.cc/5CZS-9J66].

[8] *See* Natalie Ram, *The Genealogy Site that Helped Catch the Golden State Killer is Grappling with Privacy*, SLATE (May 29, 2019, 07:30 AM), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html [https://perma.cc/E5HZ-75CA].

[9] Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database*, SLATE, (Mar. 19, 2019, 07:30 AM) https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html [https://perma.cc/293W-UFXA].

profiles to any database.[10] Rather, they were identified through the DNA samples of distant relatives who shared their genetic information on these consumer platforms.[11]

As more and more people upload their DNA into these public databases, their use in crime fighting becomes that much more potent. In one estimate, 60% of Americans from European descent are already identifiable through these familial DNA searches.[12] With at least one court already approving warrants that override private consumer DNA database privacy policies, legislative remedies will be critical to regulating how law enforcement uses these databases for fighting crime.[13] In particular, the warrantless search of these databases to apprehend criminals has raised constitutional concerns around the Fourth Amendment and genetic privacy. While the individuals who submit their DNA to these databases affirmatively volunteer their information, limiting their reasonable expectation of privacy under the third-party doctrine, the criminals themselves do not affirmatively volunteer their information. This Note will examine the current status of Fourth Amendment case law as it relates to both *Boyd's* property doctrine and the third-party doctrine to determine how courts will likely treat forensic genetic genealogical DNA testing in the future. Ultimately, I argue that criminal investigations using genetic genealogical DNA testing are not protected under the Fourth Amendment. However, the practice of extracting DNA from a suspect's abandoned property after conducting genetic genealogical searches may offer an avenue for Fourth Amendment protection.

II. TRADITIONAL DNA DATABASE SEARCH VERSUS FAMILIAL DNA SEARCHES

A. CODIS and NDIS

Traditional DNA searches in criminal investigations analyze DNA collected at crime scenes and find exact matches within both state and federally run DNA databases.[14] These databases collect DNA samples from crime scenes, felons, and arrestees.[15] CODIS is the overarching system and

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *See* Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just said Otherwise*, N.Y. TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [http://perma.cc/Z7CC-HLB7].

[14] *Familial DNA Searches*, FINDLAW (Feb. 6, 2019), https://findlaw.com/criminal/criminal-rights/familial-dna-searches.html [http://perma.cc/9GJN-73E3].

[15] *See id.*

database run by the FBI.[16] Within that system is the National DNA Index System (NDIS) that is comprised of DNA profiles contributed by federal, state, and local participating forensic laboratories.[17] When a suspected sample of the unknown perpetrator's DNA is collected, the sample is first submitted to the CODIS system. CODIS compares this sample against state databases of convicted offender and arrestee profiles.[18]

While the majority of the human genome is identical across all individuals, science has identified areas of variation, known as short tandem repeats (STRs), that contain repeating units of short three to four nucleotide DNA sequences.[19] In forensic DNA typing, between thirteen and twenty STRs are compared between the reference sample and the forensic sample.[20] In order to make a match, the lab must match the allele profile of thirteen core STRs for both the evidence and the suspect's sample. If a match is found, the lab will confirm the match and obtain the identity of the matching profile.[21] The DNA profile is also searched in the state's forensic index of unknown DNA samples collected at other crime scenes.[22] This way, a potential match can be linked to multiple crimes.[23] The system allows investigators to identify criminals, link serial violent crimes together, and even help identify missing and unidentified individuals.[24] Following the DNA Identification Act of 1994, all fifty states also participate in NDIS.[25] This means that DNA submitted to CODIS will be searched at both the state and national level.[26] As of September 2019, the NDIS contained 13,973,206 offender profiles, 3,721,360 arrestee profiles, and 973,108 forensic profiles.[27] Additionally, CODIS has produced over

---

16 *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [http://perma.cc/RHK3-JR5J].

17 *Id.*

18 *Id.*

19 Karen Norrgard, *Forensics, DNA Fingerprinting, and CODIS*, NATURE EDUC. (2008), https://www.nature.com/scitable/topicpage/forensics-dna-fingerprinting-and-codis-736/ [http://perma.cc/6KBX-UME2].

20 U.S. Dep't of Just., *Interim Policy: Forensic Genetic Genealogical DNA Analysis and Searching* (Sep. 2, 2019), https://www.justice.gov/olp/page/file/1204386/download [http://perma.cc/Z7CC-HLB7].

21 FED. BUREAU OF INVESTIGATION, *supra* note 16.

22 *Id.*

23 *Id.*

24 *Combined DNA Index System*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/QL63-L28Z].

25 FED. BUREAU OF INVESTIGATION, *supra* note 16.

26 *Id.*

27 *See CODIS – NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics

485,063 hits assisting in more than 474,576 investigations.[28] No names or other personal identifiers are stored on CODIS.[29] CODIS also removes sensitive or biomedically relevant information from samples located within the database.[30]

Familial DNA search expands the typical search parameters in CODIS to search for partial DNA matches on the theory that a partial match signals a close blood relative.[31] Instead of looking at STRs, the lab will analyze single nucleotide polymorphisms (SNPs) in genetic genealogical search.[32] SNPs span the entirety of the human genome as opposed to just one section in STR testing. SNPs are analyzed instead of STRs because SNPs allow scientists to identify shared blocks of DNA in larger blocks. The closer the family relations are, the longer the shared SNP blocks; the more distant the relations become, the shorter the shared SNP blocks.

III. THE RISE OF COMMERCIAL DNA DATABASES

A. Demographics

Familial DNA searching using consumer genetic databases is an investigative tool that is entirely separate from the FBI CODIS system.[33] Known as forensic genetic genealogy, these commercial databases are used primarily as a way for private citizens to learn more about their own genetic profiles and connect with distant relatives.[34] These commercial DNA databases have exploded in popularity over the last few years, with more than 26 million consumers volunteering their DNA to four leading commercial ancestry and health databases.[35] It is now estimated that one in twenty-five Americans now have access to their genetic data.[36] Some experts anticipate more than 100 million individuals will submit their DNA to private databases in the next two years.[37] The vast majority (nearly 80%) of individuals buying consumer DNA kits are Americans of European

[https://perma.cc/8YWX-J38Y] (Offender profiles relate to individuals currently and previously incarcerated, arrestee profiles relate to individuals who have been arrested, and forensic profiles relate to DNA samples found at crime scenes).

28 *See id.*

29 FED. BUREAU OF INVESTIGATION, *supra* note 16.

30 *See id.*

31 *See* FINDLAW, *supra* note 14.

32 FED. BUREAU OF INVESTIGATION, *supra* note 16.

33 Claire Abrahamson, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539, 2549 (2019).

34 *See id.* at 2548, 2553.

35 Regalado, *supra* note 5, at 1.

36 Abrahamson, *supra* note 33, at 2548.

37 Regalado, *supra* note 5, at 1.

descent.[38] Individuals of East Asian descent are the second most prevalent at 9%.[39] While Americans of European descent dominate the representation of commercial DNA kits, people of color are disproportionately represented in CODIS comprising over 40% of the database.[40] For many years, legal experts raised concerns that one racial population's privacy rights might be disparately impacted by DNA search, however, the rise of commercial databases has increased law enforcement's ability to access individuals and racial groups outside CODIS, mitigating some concern.[41]

B. Scope of the Data Collected

Private consumer databases capable of testing genetic samples like 23andMe and Ancestry require a saliva sample.[42] The saliva sample is used to identify SNPs. SNPs are variations in the DNA sequence responsible for genetic differences between people.[43] Unlike CODIS, commercial DNA kits test for highly personal, often medically sensitive information. Variations in the genome can be linked to recreational traits like hair curliness, preference for cilantro, as well as serious health risks like late-onset Alzheimer's disease.[44] The type of data collected by the private consumer databases depend on the type of genetic testing the database provides.[45] Most private consumer databases generally offer two types of personal genetic testing: ancestral and medical analyses.[46] 23andMe offers health reports in addition to ancestral insights.[47] Currently, it tests for two different breast cancer genes as well as a prostate cancer gene.[48] Medical testing analyzes genetic samples for genetic variants associated with certain medical conditions, while ancestral testing analyzes genetic variants to provide information on an individual's ethnic background.[49]

---

38 Abrahamson, *supra* note 33, at 2549.

39 *Id.*

40 Jason Silverstein, *The Dark Side of DNA Evidence*, THE NATION (April 15, 2013), https://www.thenation.com/article/dark-side-dna-evidence/ [https://perma.cc/JL34-CCLH].

41 *Id.*

42 Abrahamson, *supra* note 33, at 2549.

43 *Id.*

44 *Id.* at 2549.

45 *Id.* at 2550.

46 *Id.*

47 Regalado, *supra* note 5, at 4.

48 *Id.* at 5.

49 Abrahamson, *supra* note 33, at 2550.

C. Privacy Policies

Unlike CODIS, private databases are not regulated by state or federal authorities.[50] Some states do regulate genetic testing, but many of these policies do not apply to consumer databases which are generally considered recreational.[51] Additionally, these private consumer databases do not fall under the "privacy rule" of the Health Insurance Portability and Accountability Act (HIPAA) because the Act typically only applies to covered entities such as healthcare providers and insurance companies.[52] Due to this blind spot in regulatory coverage, the individual privacy policies of each company governs how the genetic data it collects is used and shared. Both 23andMe and Ancestry have policies in place to prevent law enforcement from directly accessing the data of their millions of customers. For example, 23andMe provides a guide for law enforcement to navigate its policy.[53] The guide states:

> 23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access. In certain circumstances, however, 23andMe may be required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information.[54]

As of October 2019, only ten requests had been made by law enforcement to 23andMe and 23andMe rejected each one.[55] The majority of the requests concerned credit card fraud.[56] Similarly, Ancestry's privacy policy states, "Ancestry does not voluntarily cooperate with law enforcement. To provide our Users with the greatest protection under the law, we require all government agencies . . . follow a valid legal process. . . ."[57] Ancestry also provides transparency information in regards to the number of requests is has received and responded to.[58] According to its 2018 report, Ancestry received ten valid law enforcement requests for user

---

[50] *Id.* at 2551.

[51] *Id.*

[52] *Id.*

[53] *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/799H-SP5J].

[54] *Id.*

[55] *Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ [https://perma.cc/VT8G-E7H9].

[56] *Ancestry 2019 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2019 [https://perma.cc/L8XG-ZJE7].

[57] *Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/G4SK-WX2M].

[58] *Id.*

information and provided information in response to seven of those ten requests.[59] Additionally, the requests were limited to offenses regarding credit card fraud and identity theft.[60]

In response to public outcry after the Golden State Killer case, GEDmatch updated its privacy policy to require users to affirmatively "opt-in" to their DNA being used in criminal investigations.[61] This policy drastically limited the number of profiles that could be searched; however, on November 5, 2019, a Florida judge approved a warrant to penetrate GEDmatch's entire database in a genetic genealogical search.[62] This is the first time a judge has approved of such a warrant.[63] Policy and legal experts speculate that this move could generate significant precedent and encourage other agencies to seek warrants to search GEDmatch as well as private databases such as 23andMe and Ancestry.[64]

A warrant permitting the broad-based search of a consumer genetic database suggests consumer DNA database privacy policies may be fallible after all. Even if the companies wanted to challenge the warrant, according to some experts, they may not have legal standing to do so.[65] In 2013, Facebook challenged a similar warrant on Fourth Amendment grounds and was rejected on the basis that Facebook simply stored the data and was not the subject of the criminal probe.[66] Standing further becomes an issue in challenging a warrant like the one in Florida because law enforcement rarely expects to get a perfect match from the database search. Police do not intend to find a direct match in a familial search. The goal is to identify a specific family tree and cross reference the search with other pieces of evidence as opposed to finding the suspect himself.[67]

---

[59] *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2018 [https://perma.cc/2ZNB-9YRM].

[60] *Id*.

[61] *GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm [https://perma.cc/6JTL-WVF9].

[62] Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just said Otherwise*, N.Y. TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/4MLL-ZXXV].

[63] *Id.*

[64] *Id.*

[65] Aaron Mak, *We May Be Entering a New Era for Using Consumer Genetic Information to Solve Crime*, SLATE (Nov. 8, 2019), https://slate.com/technology/2019/11/gedmatch-warrant-dna-ancestry-23andme.html [https://perma.cc/7MFD-BNBQ].

[66] *Id.*

[67] *Id.*

D. Data Ownership and Third-Party Disclosure

Both Ancestry and 23andMe explicitly state in their privacy statements that users retain ownership of the genetic information gleaned from their biological samples.[68] However, both sites also retain "the right to collect, host, transfer, process, analyze, communicate and store [genetic information]."[69] Both companies also state that by participating in the service, consumers grant the companies "a sublicensable, worldwide, royalty-free license to host, store, copy, publish, distribute, provide access to, create derivative works of, and otherwise use such User Provided Content."[70] In addition to law enforcement, Ancestry and 23andMe may, with the consent of the consumer, share data with third parties for the purposes of research. "Research" is not specifically defined in the agreement.

Because each individual consumer has an ownership right to his or her genetic information, consumers can download their genetic code as raw data and upload it to third party platforms of their own choosing. This ownership right is stipulated exclusively within consumer DNA kit privacy policies and has never been confirmed by the courts. After users download their genetic data from the database, their data is no longer protected by the database's privacy policy.[71] Many individuals choose to upload their data to public databases such as GEDmatch.com.[72] DNA located on public databases like GEDmatch can be accessed by the general public seeking familial connections as well as law enforcement using cold case DNA.

IV. PUBLIC GENETIC DATABASES

A. Use in Criminal Investigations

When law enforcement uses genealogy databases to search for DNA matches, it conducts what is known as a "long-range familial search."[73] These long-range searches use DNA samples to partially match the sample

---

[68] *Ancestry Privacy Statement*, ANCESTRY (May 19, 2021), https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/9NLX-TKL8]; *see also*, *23andMe Privacy Statement*, 23ANDME (May 19, 2021), https://www.23andme.com/about/privacy/ [https://perma.cc/7YS6-592V].

[69] *See e.g.*, *Ancestry Terms and Conditions*, ANCESTRY (May 10, 2021), https://www.ancestry.com/cs/legal/TermsAndConditions [https://perma.cc/4ESR-4AS3].

[70] *Id.*

[71] *Id.*

[72] *GEDmatch Get Started – or Get Alternatives*, YOUR DNA GUIDE (last visited December 17, 2019), https://www.yourdnaguide.com/upload-to-gedmatch [https://perma.cc/FRQ4-6MRD].

[73] Abrahamson, *supra* note 33, at 2553.

to typically distant relations such as second and third cousins.[74] A 2018 study concluded that "around 60 percent of Americans of European descent could be matched to a third cousin or closer relation," even if they have not taken the test.[75] Parabon Nanolabs is the most widely recognized forensic consulting firm in the world.[76] The firm gained its recognition by using DNA databases such as GEDmatch to generate leads to crimes and track down offenders.[77]

GEDmatch is a free, open-source database that allows genealogists to compare segments of DNA.[78] The segments can be cross-matched with family trees and public records to identify distant relations to the source DNA.[79] GEDmatch users voluntarily upload their raw DNA data (often created by sites like 23andMe and Ancestry) and GEDmatch matches their data to potential relatives.[80] Initially, use of GEDmatch's database was accessible by law enforcement.[81] This allowed law enforcement to anonymously upload cold case DNA samples and search for matches. The landmark example of this technique was in the Golden State Killer case.[82]

For decades, the DNA of the suspected Golden State Killer, a criminal linked to twelve homicides and forty-five violent rapes between 1976 and 1986, sat in evidence storage.[83] It was not until 2018 when investigators ran a DNA sample of the suspected killer through GEDmatch's public database that they got their first break in the case.[84] Using GEDmatch, a genetic

---

74 *Id.*

75 Brian Resnick, *How Your Third Cousin's Ancestry DNA Test Could Jeopardize Your Privacy*, VOX (Oct. 15, 2018, 10:20 AM), https://www.vox.com/science-and-health/2018/10/12/17957268/science-ancestry-dna-privacy [https://perma.cc/C2B4-DPNB]; *see also The Controversial Company Using DNA to Sketch the Faces of Criminals*, NATURE (May 19, 2021), https://www.nature.com/articles/d41586-020-02545-5 [https://perma.cc/4X2C-33Q7].

76 NATURE, *supra* note 75.

77 *Id.*

78 Resnick, *supra* note 75; Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database: "I never expected anything like this,"* THE ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695/ [https://perma.cc/UGJ9-C6TC].

79 Zhang, *supra* note 78.

80 Sarah Zhang, *The Messy Consequences of the Golden State Killer Case*, ATLANTIC (Oct. 1, 2019), https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/ [https://perma.cc/6PWD-M7EQ].

81 NATURE, *supra* note 75.

82 Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 27, 2018, 8:50 AM), https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/ [https://perma.cc/3DYR-XRDU].

83 *Id.*

84 *Id.*

geneaologist hired by law enforcement identified two GEDmatch profiles who looked to be distant cousins of the Golden State Killer.[85] Using these matches, the genealogist constructed a family tree that placed three potential suspects in California at the time of the Golden State Killer's crime spree.[86] Law enforcement acquired a cigarette discarded by one suspect, and it was a match.[87] Police arrested Joseph DeAngelo on April 24, 2018.[88] It was the first criminal case to be solved using the technique.[89]

Since the capture of the Golden State Killer, GEDmatch has played a role in identifying at least thirty-nine additional cold case arrests and twelve unidentified remains.[90] Parabon NanoLabs has played a critical role in assisting law enforcement with genetic genealogical search techniques.[91] Through the company's genetic genealogy unit, "analysts compare crime scene DNA samples against public genetic genealogy databases to narrow down a suspect list to a region, a family, or even an individual."[92] Further, when this strategy is insufficient, Parabon deploys additional tools to help investigators.[93] One tool is called "Snapshot DNA Phenotyping" which identifies physical attributes (phenotypes) in the unknown DNA sample and builds a physical composite from the DNA sample.[94] This tool can be used to help law enforcement to talk with members of the community in target regions with a more accurate physical description.[95] The current technology can only produce rough pictures good enough to narrow a manhunt or eliminate possible suspects.[96] The second tool is called the

---

85 NATURE, *supra* note 75.

86 *Id.*

87 *Id.*

88 *Id.*

89 *Id.*

90 *Message about the Recent Changes at GEDmatch*, DNA DOE PROJECT (May 19, 2021) https://dnadoeproject.org/message-about-the-recent-changes-at-gedmatch/ [https://perma.cc/63ES-SFU4].

91 Selk, *supra* note 82.

92 *Parabon Announces Snapshot Genetic Genealogy Service for Law Enforcement*, PARABON-NANOLABS (May 8, 2018), https://parabon-nanolabs.com/news-events/2018/05/parabon-snapshot-genetic-genealogy-dna-analysis-service.html [https://perma.cc/D75J-8QAX].

93 *Id.*

94 *Id.*

95 *Id.*

96 This particular feature has been most prominently used in China as part of its mass DNA collection effort from hundreds of Uighurs—an ethnic minority in the Xin Jiang province. Experts worry that the technology is being developed in order to justify and intensify intense racial profiling and state discrimination of the Uighurs in the region. In the long term, this technology may be able to integrate with the state's highly developed facial recognition systems to tighten state surveillance efforts. Sui-Lee Wee & Paul Mozur, *China Uses DNA to Map Faces, With Help From the West*, N.Y. TIMES (December 3, 2019), https://www.nytimes.com/2019/12/03/business/china-dna-uighurs-

"Snapshot Kinship Inference" service that accurately predicts the relationship between two DNA samples and helps investigators include or exclude branches of large family trees by testing family members.[97]

The use of genetic genealogy searching in law enforcement is still relatively new, having never been tested in court until June 2019 in the conviction of William Talbott II in the 1987 double murder of a young Canadian couple in Washington state.[98] The defense never challenged the use of genetic genealogy on privacy grounds, nor did it pose a single question about the technique.[99] Two days into deliberation, the jury returned a guilty verdict on two counts of homicide.[100] In June of 2019, Jesse Bjerke was charged with the violent rape of a woman at a pool after his DNA was identified through genetic genealogical search.[101] Parabon Nanolab's genetic genealogical search matched Bjerke's DNA to two cousins on both sides of his family.[102] Using this data, law enforcement narrowed their search to Bjerke based on his appearance and his whereabouts the time the rape occurred.[103] They began tailing him and retrieved a straw he used at a restaurant from the garbage. The result was a one in 7.2 billion chance the DNA was not his.[104] Bjerke would later plead guilty to the charge and is still awaiting sentencing.[105]

B. Privacy Policies Post-Golden State Killer

Amidst public outcry over privacy concerns, GEDmatch published a new privacy policy requiring users to affirmatively opt-in to allow their genetic data to be used in criminal investigations.[106] The policy move has since dramatically reduced the number of profiles available to the police

xinjiang.html?te=1&nl=morning-briefing&emc=edit_NN_p_20191203. [https://perma.cc/6Q5F-T93M].

97 *Snapshot Kinship Inference*, PARABON-NANOLABS, https://snapshot.parabon-nanolabs.com/kinship [https://perma.cc/Z46R-87GV].

98 *See* Heather Murphy, *Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One*, N.Y. TIMES (July 1, 2019), https://www.nytimes.com/2019/07/01/us/dna-genetic-genealogy-trial.html [https://perma.cc/4EFX-VEQ9].

99 *Id.*

100 *Id.*

101 Rachel Weiner, *Alexandria Rape Suspect Challenging DNA Search Used to Crack Case*, WASH. POST (June 10, 2019), https://www.washingtonpost.com/local/public-safety/alexandria-rape-suspect-challenging-dna-search-used-to-crack-case/2019/06/10/24bd0e34-87a5-11e9-a870-b9c411dc4312_story.html?noredirect [https://perma.cc/8P9X-8N56].

102 *Id.*

103 *Id.*

104 *Id.*

105 *Id.*

106 *See* GEDMATCH, *supra* note 61.

from approximately 1.3 million to 160,000.[107] In response, competing public databases such as FamilyTreeDNA has marketed its database to users as a way to help law enforcement catch criminals.[108] When the company discovered the FBI had been quietly using the site to upload genetic profiles from crime scenes, it changed its terms and services to explicitly permit law enforcement to use the database in cases of violent crimes without notifying its customers.[109] Less than 1% of FamilyTreeDNAs users elected to opt out of law enforcement after one week of the policy being in place.[110] FamilyTreeDNA's current law enforcement guidelines require law enforcement to register the sample and request permission to use the platform, but does not require an official warrant to conduct genetic genealogy searches on the site.[111] As of July 22, 2019, the FamilyTreeDNA database contained a total of 1,070,210 records.[112] A recent survey conducted by Baylor University asked participants about law enforcement's use of these databases.[113] Of the 1,587 respondents, 91% supported the use of forensic genealogy for violent crimes, and 46% supported its use for nonviolent crimes.[114] While the sample size was relatively small, the survey seems to reflect some level of societal acceptance for using genetic genealogical testing for crime fighting.

V. FOURTH AMENDMENT DOCTRINE

A. Property Doctrine and Reasonable Expectations Analysis

The Fourth Amendment of the U.S. Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[115]

---

107 Zhang, *supra* note 80.

108 Sarah Zhang, *A DNA Company Wants You to Help Catch Criminals*, ATLANTIC (Mar. 29, 2019), https://www.theatlantic.com/science/archive/2019/03/a-dna-company-wants-your-dna-to-catch-criminals/586120/ [https://perma.cc/3JQC-PAM5].

109 *Id.*

110 *Id.*

111 *Id.*

112 *Why Choose FamilyTreeDNA*, FAMILYTREEDNA (last visited December 17, 2019), https://www.familytreedna.com/why-ftdna (last visited May 23, 2021).

113 *Id.*

114 *Id.*

115 U.S. CONST. amend. IV.

The Fourth Amendment is the source of the United States' privacy protections.[116] As early as 1886, the Supreme Court has recognized the need to protect the "sanctity of a man's home and the privacies of life."[117] The Fourth Amendment also establishes guidelines for law enforcement and police activity on both a state and federal level.[118] The Fourth Amendment was constructed as a response against general "writs of assistance" common under British colonial rule that allowed British law enforcement to "draft assistance . . . and to search any place smuggled goods might be concealed."[119] In *Boyd v. United States*, the Court held that the Fourth Amendment applied to "all invasions on the part of the government and its employees on the sanctity of a man's home and the privacies of life."[120] Further, the *Boyd* Court interpreted the Fourth and Fifth Amendments in tandem stating:

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense . . . but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgement. In this regard the fourth and fifth amendments run almost into each other.[121]

Boyd defined Fourth Amendment jurisprudence in terms of an individual's property interest.[122] As America developed, the public demand for government control increased at the same time the fundamental right to privacy gained acceptance, and the impact of a strict interpretation of *Boyd* on the ability to acquire important evidence began to produce undesired results.[123] As a result, *Boyd's* property doctrine became less and less relevant.[124]

In an effort to protect people and not just places, the Supreme Court shifted Fourth Amendment doctrine from a property tort-based approach in *Boyd v. United States* to a reasonable expectations analysis in *Katz v. United States*.[125] *Katz* addressed Fourth Amendment concerns around

---

116 RONALD JAY ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 321 (2016).

117 *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

118 *Id.*

119 *Id.* at 339.

120 *Id.* at 298.

121 *Id.*

122 *See id.*

123 *See id* at 303–05.

124 *See id.* at 334.

125 *See generally* Katz v. United States, 389 U.S. 347, 359 (1967).

increasingly sophisticated government surveillance techniques.[126] *Katz* explored whether the government could wiretap a telephone booth to record a defendant's conversations without first obtaining a warrant. The Court held in favor of the defendant, and in Justice Harlan's landmark concurrence, he defined a new standard for judging reasonable search and seizure.[127] Justice Harlan stated, "the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[128] The Court highlighted how advancing technology, such as electronic surveillance, "violated the privacy upon which he justifiably relied while using a telephone booth, and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[129]

The reasonable expectations standard has continued to prevail in modern Fourth Amendment jurisprudence, but there is some division as to whether the *Katz* opinion effectively overruled *Boyd's* property doctrine. *United States v. Jones* reinvigorated previously abandoned property interest rationales in 2012. In *Jones*, the Supreme Court stated that *Katz* did not replace traditional conceptions of Fourth Amendment protection and property interests.[130] The *Jones* Court stated, "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates. *Katz* did not repudiate that understanding."[131] The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test.[132] For the first time since *Katz*, the Court confirmed that the Fourth Amendment's original protections of individual property interests were relevant. *Jones* indicated that while Fourth Amendment property doctrine was by no means a dominant force in Fourth Amendment jurisprudence, it may still be relevant in cases when the government interacts with individual property for the purposes of surveillance.[133]

---

126 ALLEN ET AL., *supra* note 116, at 367–68.

127 *See generally Katz*, 389 U.S. at 359 (1967).

128 *Id.* at 365 (Harlan, J., concurring) (internal quotation marks omitted).

129 *Id*. at 389.

130 *See* United States v. Jones, 565 U.S. 400, 406–07 (2012).

131 *Id.*

132 *Id.*

133 *See generally id*.

B. Third-Party Doctrine

The third-party doctrine was first articulated in *United States v. Miller* as a way to clarify the reasonable expectations analysis established in *Katz*.[134] Specifically, the court held that an individual loses a reasonable expectation of privacy under the Fourth Amendment when the individual volunteers information to a third party. In the case of *Miller*, the court refused to extend Fourth Amendment protection to a plaintiff's bank records.[135] Any question of whether the third-party doctrine would be a permanent staple in Fourth Amendment jurisprudence was eliminated three years later when the Supreme Court handed down *Smith v. Maryland*. In this case, the government's interception of a phone number dialed by the defendant using a pen register constituted a reasonable search under the *Katz* test because the defendant had no reasonable expectation of privacy when he volunteered the information to the phone company.[136] The Court explained, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.[137] This rationale is based on the idea that when an individual assumes the risk in revealing his or her personal details to another person or entity, that information need not be privileged from government seizure.[138]

The third-party doctrine has been repeatedly upheld with few limits until the Supreme Court's recent opinion in *Carpenter v. United States*. In *Carpenter*, the Court distinguished cell site location data from information affirmatively volunteered to third-parties encompassed in the third-party doctrine.[139] The Court echoed sentiments raised in *Jones*, arguing that *Katz's* reasonable-expectation-of-privacy test does not supplant the basic principles that underpin the Fourth Amendment.[140] The *Carpenter* Court reinvigorated originalist Fourth Amendment principles in stating the "central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance'" and "to secure 'the privacies of life' against 'arbitrary power.'"[141] Regarding affirmative consent, the *Carpenter* Court argued the cell phone has become ubiquitous to modern life, and users have no control over how their location data is used by third-party

134 *See generally* United States v. Miller, 425 U.S. 435, 437 (1976).

135 *Id*.

136 Smith v. Maryland, 442 U.S. 735, 743 (1979).

137 *Id.* at 743.

138 *Miller*, 425 U.S. at 443.

139 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

140 *Id*. at 2213.

141 *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948) and Boyd v. United States, 116 U.S. 616, 630 (1886)).

cell phone companies.[142] Stuck between the third-party doctrine articulated in *Smith* and *Miller* and the property interest doctrine reinvigorated in *Jones*, the *Carpenter* Court declined to apply the third-party doctrine to cell site location data, and indicated that it would be limited in cases where technological advancement had created a reasonable expectation of privacy and a lack of affirmative consent in how individual data would be used.[143]

C. Fourth Amendment protections of biological property

In 2013, the Supreme Court considered how much leeway the Constitution gives police to adopt new DNA technology for crime solving in *Maryland v. King*. In 2009, Alonzo King was arrested for first- and second-degree assault.[144] "As part of a routine booking procedure," his DNA was taken by cheek swab, known as a buccal swab, and entered into law enforcement's CODIS system.[145] His DNA matched the DNA taken from a rape victim in a case that had previously been unsolved.[146] Alonzo King was subsequently charged and convicted of the rape. The case turned on whether the mandatory DNA collection constituted an unreasonable search and seizure. In a close 5-4 opinion, the Supreme Court held against King, ruling when officers make an arrest supported by probable cause and bring that suspect into custody, analyzing a cheek swab is a legitimate booking procedure under the Fourth Amendment. [147]

The Court's analysis followed the familiar balancing test framework that requires the court to balance the interests of the state against the privacy interests of the individual.[148] The court analogized DNA collection to typical booking procedures such as fingerprinting that are used to identify the criminal and inform law enforcement of any past convictions.[149] Justice Scalia, joined by Justices Ginsburg, Sotomayor, and Kagan, issued a poignant dissent, arguing the scope of the holding rested on an unenforceable principle.[150] The dissent recognized that without concrete limiting principles, DNA identification would eventually be used to identify individuals for minor offenses such as traffic violations.[151] The dissent also reasserted the purpose of the Fourth Amendment stating, "[t]he

142 *Id.* at 2218.
143 *Id.*
144 Maryland v. King, 569 U.S. 435, 440 (2013).
145 *Id.* at 441, 444–45.
146 *Id.* at 440.
147 *Id.* at 465–66.
148 *Id.* at 444–45.
149 *E.g.*, *id.* at 451.
150 *Id.* at 481 (Scalia, J., dissenting).
151 *Id.*

Fourth Amendment forbids searching a person for evidence of a crime when there is no basis for believing the person is guilty of the crime or is in possession of incriminating evidence. That prohibition is categorical and without exception . . . ."[152]

Critics of the case argue that the *King* Court relied on the wrong line of cases by comparing DNA sampling to fingerprinting. A better comparison, one critic argues, was a line of cases involving the search of information on seized computers.[153] "A search of someone's DNA is unique with respect to the physical intrusion necessary to effectuate the search and the amount of data rendered by the search."[154] Especially when familial and genetic genealogical testing is considered, this type of testing reveals far more than mere identification.[155]

VI. POLICY DEVELOPMENTS IN FORENSIC GENETIC GENEALOGICAL TESTING

A. Legislative

There is no national standard for familial DNA testing, but US prosecutors have looked to the United Kingdom's DNA profiling system as a potential model for US enforcement.[156] Twelve states currently authorize familial DNA testing, and two jurisdictions, Maryland and Washington, D.C., have specifically prohibited familial DNA testing.[157] US jurisdictions typically impose strict requirements in order to use familial search.[158] These requirements typically limit the use of familial searches to violent crimes that cause serious injury, death, or cases that present a "continuing threat of imminent and serious harm to the community, which remain unsolved after exhausting traditional investigative leads. . . ."[159] Additionally, most states require a "sample requirement," meaning that the unknown sample must be a complete profile from a single source.[160] Finally, the familial search must

---

[152] *Id.* at 466.

[153] Stephanie B. Noronha, Comment, Maryland v. King*: Sacrificing the Fourth Amendment to Build Up the DNA Database*, 73 MD. L. REV. 667, 668 (2014).

[154] *Id.*

[155] *Id.* at 693.

[156] Mary McCarthy, *Am I My Brother's Keeper?: Familial DNA Searches in the Twenty-First Century*, 86 NOTRE DAME L. REV. 381, 394 (2011).

[157] Victoria Romine, *Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe*, 53 ARIZ. ST. L.J. 367, 378 (2021).

[158] *Id.*

[159] Alexandra Nieto, *Familial Searching: How Implementing Minimum Safeguards Ensures Constitutionally-Permissible Use of This Powerful Investigative Tool*, 40 CARDOZO L. REV. 1765, 1772 (2019).

[160] *Id.* at 1772–73.

usually be approved by the state's Attorney General, who signs off on the application and approves the case as qualifying for a familial search.[161] Familial DNA searches within the public databases are highly regulated and limited in their jurisdictional application. However, private commercial databases offer law enforcement the opportunity to leverage familial DNA searches without the same regulatory hurdles.

If courts and privacy policies are not a viable way to challenge law enforcement access to consumer databases and genetic genealogical search, legislation will be a critical avenue for genetic privacy advocates.[162] The rise of DNA big data and genetic genealogical testing raises issues around whether the US is adequately protecting consumers.[163] Law professors, doctors, and other genomics experts have raised concerns that because laws regulating genetic privacy are varied across federal agencies and states, there is no guarantee of genetic anonymity.[164] As a result, a group of advocates led by Professor Susan Wolf at the University of Minnesota have developed a public database for genomics law called LawSeq.[165] The database compiles all federal and state laws, regulations, official guidance, and professional standards that regulate the field of genomics. The group is also working to make recommendations to policymakers on how to legislate around DNA data.

B. Interim DOJ Guidance

While the United States has reached some consensus on DNA data and health privacy, forensic searches are still varied depending on subject matter and location. In an effort to offer some standardization, the Department of Justice (DOJ) has released an interim policy that could help standardize how forensic genetic genealogical testing is handled in federal cases. Federal agencies are quickly adapting to the use of genetic genealogical search in criminal investigations.

On November 11, 2019, the DOJ published an interim policy on the use of forensic genetic genealogical DNA analysis and searching in criminal investigations.[166] The purpose of the policy is to promote reasoned

---

161 *Id.* at 1773.

162 Aaron Mak, *We May Be Entering a New Era for Using Consumer Genetic Information to Solve Crime*, SLATE (Nov. 8, 2019, 4:01 PM), https://slate.com/technology/2019/11/gedmatch-warrant-dna-ancestry-23andme.html [perma.cc/DD55-YQAT].

163 Megan Molteni, *The U.S Urgently Needs New Privacy Laws*, WIRED (May 1, 2019, 8:00 AM), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/ [perma.cc/J85D-RVTC].

164 *Id.*

165 *Id.*

166 U.S. Dep't of Just., *supra* note 20, at 7.

and responsible usage of the technology. The policy only applies to criminal investigations which the DOJ has exclusive or concurrent jurisdiction. First, the DOJ limits the use of genetic genealogy search to violent crime defined as homicide and sex crime.[167] The sample must also be from a putative perpetrator. A "putative perpetrator" is defined by the DOJ as a "one or more criminal actors reasonably believed by investigators to be the source of, or a contributor to, a forensic sample deposited during, or incident to, the commission of a crime."[168] Law enforcement can also use genetic genealogical testing to identify unidentified human remains from suspected homicide cases.[169]

Next, the DOJ imposes significant limitations on how the results of genetic genealogical search can be used. Matches can only be used as an investigative lead, and further investigation is needed to meet the requirements for an arrest.[170] Genetic genealogical testing can only be used after other databases like CODIS have been searched and other traditional investigation methods have been deployed.[171]

Further, law enforcement agencies are no longer permitted to act covertly when using public databases. They must identify themselves as law enforcement.[172] When a database search and subsequent genealogical research reveals third parties not in the database with a closer genetic kinship to the sample DNA, law enforcement must seek informed consent before any samples are collected from third parties.[173]

Finally, law enforcement is required to keep all data confidential. If a suspect is charged before genetic genealogical testing is complete, law enforcement is required to cease testing. If a suspect is charged with a crime after genetic genealogical testing is done, the investigative agency must request that all profiles and genetic information be removed from records and provided directly to the investigative agency so that they may be retained for prosecution and judicial proceedings.[174]

---

167 *Id.* at 4.
168 *Id.*
169 *Id.*
170 *Id.*
171 *Id.* at 7.
172 *Id.* at 6.
173 *Id.*
174 *Id.*

VII. ANALYSIS

A. Warrantless Genetic Genealogical Search and the Fourth Amendment

Under the reasonable-expectation-of-privacy test established in *Katz* and the updated third-party doctrine analysis defined in *Carpenter*, the Fourth Amendment offers no protection for suspects identified through genetic genealogical search. In *Guilt by Genetic Association*, Abrahamson argues that *Carpenter* holds the third-party doctrine will not be applied to information databases with a reach that could permit the government to surveil a vast majority of United States citizens.[175] However, *Carpenter's* holding seems to turn more critically on both the lack of affirmative consent in volunteering cell tower location data and the essentiality of smart phones to modern life. The case does not contemplate the scope of the government's ability to surveil its citizens. Consumer DNA databases are easily distinguishable from the databases contemplated in *Carpenter* because users affirmatively volunteer their genetic information, whereas consumers do not affirmatively consent to giving cell phone location data to third parties.[176] The affirmative consent issue in genetic genealogical search does have some differences than a typical third-party doctrine issue under *Carpenter*. The fact that individuals share similar sequences of DNA operates as a kind of loophole for the third-party doctrine because an individual may never consent to being identified in a consumer database, nor have a reasonable expectation that he might be identified. While this issue stands out as different than other third-party doctrine issues, Fourth Amendment protections will continue to fall away under *Katz* and the third-party doctrine in genetic genealogical search without a different interpretation of the affirmative consent rule.

Familial DNA testing has been in practice since 2008, and twelve of the most populous and racially diverse states currently allow it.[177] Nearly all state policies impose limits on when familial DNA testing can be used.[178] Suspect DNA samples taken from violent crime scenes and entered into long range familial DNA searches are justified under the Fourth Amendment because there is a strong government interest in public safety. This interest is affirmed in cases such as *Maryland v. King* where the Court identified a governmental interest in the identification of suspects brought into custody under probable cause. Furthermore, familial DNA searches

---

175 Abrahamson, *supra* note 33, at 2559–60.

176 *See* Rebecca Gold, *From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges*, 55 CAL. W. L. REV. 491, 511 (2019).

177 Romine, *supra* note 157, at 378.

178 *Id.*

rarely reveal direct matches. The technique simply serves to narrow the field of suspects, and more traditional investigative work is required to criminally charge a suspect.

A traditional reading of *Boyd* may offer Fourth Amendment protection against warrantless genetic genealogical search, but modern case law has not embraced a stricter reading of *Boyd*. Under *Boyd*, the Fourth Amendment protects an individual's "indefeasible right of personal security, personal liberty, and private property."[179] It might be argued under *Boyd* that an individual's sense of personal security is violated through genetic genealogical search. Individuals have no control over their relative's choice to submit their DNA to a database, and this lack of control over one's own property interest and the state's ability to identify a specific individual may violate a reasonable expectation of personal security.

Jones is the most recent case to reinvigorate originalist definitions of privacy established in *Boyd* by suggesting that the Fourth Amendment should be understood as the "preservation of th[e] degree of privacy against government that existed when the Fourth Amendment was adopted."[180] *Jones* held that a GPS tracking device installed on the bottom of a suspect's vehicle constituted an unlawful warrantless search of a citizen's property. The Court characterized the GPS tracking device as the government "physically occup[ying] private property for the purpose of obtaining information."[181] There is no direct application of *Jones* to warrantless genetic genealogical database searches, but it elevated *Boyd's* concept of property rights in the analysis of Fourth Amendment protections.

In *Maryland v. King*, the Court categorized DNA as a type of personal property within the meaning of the Fourth Amendment.[182] This categorization is best applied under *Jones* within the context of DNA seized at crime scenes. DNA and other biological property left at crime scenes is no longer protected under the Fourth Amendment once there is a warrant to investigate and collect evidence at a crime scene. When characterized this way, the process of genetic genealogical search operates the same way as using any kind of evidence to narrow potential perpetrators. Genetic genealogical search narrows the pool of potential suspects using the suspect DNA extracted as evidence from the crime scene. Law enforcement must go beyond genetic genealogical search using

---

179 ALLEN ET AL., *supra* note 116, at 281 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

180 United States v. Jones, 565 U.S. 400, 406 (2012) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

181 *Id.* at 404.

182 *See generally*, Maryland v. King, 569 U.S. 435, 456 (2013).

other tactics such as extracting suspect DNA from abandoned property to match the cold case DNA to a potential suspect.

B. Forensic DNA extraction from abandoned property

Genetic genealogical search has one powerful limitation: Its purpose is not to identify a suspect. It can only narrow the suspect pool to familial connections. In every case where genetic genealogical testing was used, suspect identification required law enforcement to extract DNA from abandoned or unattended property belonging to the suspect. In many of the cases, no warrant was required to extract the DNA. The Supreme Court has never ruled on whether DNA extracted from trash requires a warrant. This aspect of genetic genealogical search technique is the most susceptible to a possible Fourth Amendment violation. In *California v. Greenwood*, the Court argued "[t]he warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable."[183] Under the reasonable-expectation-of-privacy test, the Court heavily relied on both *Smith* and *Katz* to establish that it was custom to hand over garbage to a third party, and even allow third parties to take ownership over that garbage. For this reason, the discarding of garbage on the curb is protected under the third-party doctrine and removes any reasonable expectation of privacy.

The extraction of highly personal, private information found on the human genome can be distinguished from the types of evidence the court considered acceptable in *Greenwood*. At one point, the Court stated, "police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Hence, '[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'"[184] Like cell site location data, DNA matter, even when discarded, is not something individuals knowingly and voluntarily display to the public. There is an expectation that our genetic information and everything contained within it is sensitive, private, and not accessible to the average citizen. DNA is invisible to the naked eye, and impossible to decode without sophisticated technology. Therefore, under a *Carpenter* third-party doctrine analysis, DNA extraction from suspect trash may be protected under the Fourth Amendment. Similar to cellular location data, it

183 California v. Greenwood, 486 U.S. 35, 39 (1988).

184 *Id.* at 41 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

is impossible for humans to choose whether their DNA is left in trash. DNA falls off of humans every minute of every day, yet we retain the reasonable expectation that this aspect of our lives be kept private. There is a lack of voluntariness in DNA found within trash that is sufficient to be protected under the Fourth Amendment.

Jones is not directly on point in addressing the issue of DNA extracted from suspect trash. Trash by definition assumes discarded property is no longer under the ownership of the individual. However, DNA is a form of biological property, and because DNA is an extension of an individual's personhood, it could be argued under *Jones* that DNA ceases to become trash when it is separated from discarded objects and becomes an individual's private property interest protected under the Fourth Amendment.

While leveraging familial DNA search techniques in public DNA databases clearly falls outside the scope of Fourth Amendment protections, the investigative practice of identifying a suspect through genetic genealogical search and subsequently warrantlessly extracting suspect DNA from abandoned or unattended property does trigger Fourth Amendment protections under a *Carpenter* third-party doctrine analysis.

CONCLUSION

Technological innovation has dramatically shifted what society considers private and how personal information is shared, but the core intent of the Fourth Amendment remains. It protects people from unreasonable search and seizure, but it does not protect people from lack of foresight in when they choose to share their data and personal information on the internet. Sharing genetic information for the express purpose of being found by family members in public DNA databases forecloses the possibility of Fourth Amendment protections under the third-party doctrine, all but securing a searchable genetic panopticon built by a civilian population without any help from the state. While the Fourth Amendment should protect against the extraction of DNA from trash or abandoned property *after* a genetic genealogical search has taken place, our society is still tasked with reconciling how our legislatures will protect our own privacy interests in an age where our DNA is no longer anonymous.